Privacy Guide

A guide to complying with privacy laws in Australia

Sep 2024

justice connect

Contents

Introduction **4**

Part 1 **7**

What information is covered by Privacy Laws? **8**

What is 'personal information'? 8

What is sensitive information? 10

What is 'health information'? 10

Other categories of confidential information 11

Part 2 **12**

Is your organisation subject to Privacy Laws? **13**

Federal Privacy Laws: Australian Privacy Principles (APPs) 14

Exemptions to the APPs 16

State and territory Privacy Laws and Principles 18

Health Privacy Laws 19

Part 3 **20**

What are your organisation's obligations under Privacy Laws? **21**

Your organisation's privacy policy 22

Rules for collecting information 23

Collecting personal information 23

Collecting sensitive and health information 24

Things you are obliged to tell the person providing information 26

Getting consent 27

Unsolicited information 28

Storing personal information 29

Security measures 29

Other recommended action 30

Health information 30
Using or disclosing information 31
Direct marketing 32
Access to and correcting personal information 33
Disclosing across borders 33
Responding to a privacy breach 34
When must you report a breach? 34
Has a notifiable data breach occurred? 34
Making mandatory notifications 35
Managing actual and suspected breaches 35
What happens if your organisation doesn't comply with Privacy Laws? 35
Ongoing obligations 36
Comparison of Commonwealth and State and Territory Privacy Principles 37

Part 4 **41**

Fundraising and privacy 42
Privacy issues when fundraising 42
Private ancillary funds 43

Part 5 **44**

Practical tips for complying with Privacy Laws 45
Practical tips 45
'Permitted situations' – quick reference guide 46

Introduction

This guide is for not-for-profit organisations in Australia who want to understand more about their obligations under privacy laws in Australia.

Disclaimer

This guide provides information on privacy laws for community organisations. This information is intended as a guide only and is not legal advice. If you or your organisation has a specific legal issue, you should seek legal advice before deciding what to do.

Please refer to the full disclaimer that applies to this guide.

Privacy laws

This guide describes obligations under the following legislation, collectively called **Privacy Laws**:

Privacy Laws
Commonwealth *Privacy Act 1988* (Cth) (**Privacy Act**) which includes the Australian Privacy Principles (**APPs**)
Australian Capital Territory *Information Privacy Act 2014* (ACT) *Health Records (Privacy and Access) Act 1997* (ACT)
New South Wales *Privacy and Personal Information Protection Act 1998* (NSW) *Government Information (Public Access) Act 2009* (NSW) *Health Records and Information Privacy Act 2002* (NSW)

Northern Territory

Information Act 2002 (NT)

Queensland

Information Privacy Act 2009 (QLD)

Tasmania

Personal Information Protection Act 2004 (Tas)

Victoria

Privacy and Data Protection Act 2014 (Vic)

Health Records Act 2001 (Vic)

South Australia and **Western Australia** don't currently have a legislative scheme for privacy law.

Note, however:

- in **South Australia**, an administrative direction on handling personal information binds the public service (PC012- Information Privacy Principles (**IPPs**) Instruction), and
- the **Western Australian** Government tabled the *Privacy and Responsible Information Sharing Bill 2024* in May 2024, which will (if passed) establish information privacy principles that apply to the handling of personal information by Western Australian public entities

Does your organisation use, store or disclose information about people?

If you work for a not-for-profit organisation, it's likely that you or your colleagues collect, use, store or disclose information about people – for example, when you deliver services or gather new membership information. This information will often be classified as 'personal information' under Privacy Laws and may include 'sensitive information' or 'health information'. 'Sensitive information' and 'health information' are subcategories of personal information that require special treatment.

You must consider your organisation's responsibilities under Privacy Laws when you deal with personal information. This includes when you:

- engage and manage employees and volunteers
- advertise your products and services
- fundraise and communicate with members and the public,
- or store and manage records

Note

Handling personal information in a lawful, transparent and respectful way is an important part of building the trust of the people your organisation works with, as well as avoiding any legal consequences of a data breach, including financial penalties.

Questions for your organisation to consider

This guide helps your not-for-profit organisation understand its Privacy Law obligations by considering the following questions:

1.	What kinds of information do Privacy Laws cover?
2.	Is the information our organisation collects and holds covered by Privacy Laws?
3.	Which Privacy Laws apply to our organisation?
4.	How do I apply the Privacy Law requirements to my not-for-profit organisation?

This guide also:

- considers specific requirements for privacy policies and the treatment of personal information in fundraising, and
- includes practical tips and links to more information

Caution

The information in this guide is of a generic nature only and should not be relied on as specific advice. Rather, it provides an overview of the Commonwealth and state and territory laws on privacy. The content is also subject to change.

Privacy Laws are complex and not always easy to apply in practice. You should seek your own legal and other advice for any question, or for any specific situation or proposal, before making any final decision.

Part 1

What information is covered by Privacy Laws?

What information is covered by Privacy Laws?

This part covers:

- personal information
- sensitive information
- health information
- other categories of information

Generally, Privacy Laws do not regulate or apply to all the information your organisation collects or deals with.

So, the first step in understanding your obligations under Privacy Laws is to determine whether the information you hold, or want to collect, falls into one of the following categories:

1.	**personal information**
2.	**sensitive information**
3.	**health information**

Privacy Laws apply to these categories in different ways. The way that Privacy Laws apply to your organisation also depends on the size and type of your organisation (discussed further in part 2 of this guide).

What is ‘personal information’?

‘Personal information’ is information or an opinion about an identified person (or a person who is ‘reasonably identifiable’).

Personal information can be:

- true or false
- verbal, written or photographic, or
- recorded or unrecorded

Personal information includes a person’s name, address, contact details (such as telephone number or email), date of birth, gender, sexuality and race.

When will someone be ‘reasonably identifiable’?

Whether someone is ‘reasonably identifiable’ from the information you hold depends on:

- the nature and extent of the information
- how the information was received, and
- whether it’s possible for you to identify the person from resources you hold (including other information available to you)

Deceased people don’t have ‘personal information’ under federal Privacy Laws. But, under some state and territory laws, a deceased person’s personal information may still be protected for a period. Also, where information about a deceased person includes information about a living person (for example, if a deceased person with children has an inheritable medical condition) this information may form personal information about the living person.

Personal information doesn’t include:

- anonymous information
- aggregated information (for example, data that reflects trends without identifying the sample)
- de-identified information not reasonably capable of re-identification, or
- information about companies or other entities which does not identify individuals

Example

Consider a car licence plate. Most people can’t identify the owner of a car simply from the registration number. So, to most people, knowing a car’s licence plate number wouldn’t make the car owner ‘reasonably identifiable’.

But if you work for a car registration agency, you may be able to identify the owner of the car because you have access to other information. Holding information about the car registration would make the person ‘reasonably identifiable’ to you from the information you hold. In these circumstances, the registration number would be considered personal information.

Tips

- The definition of ‘personal information’ is very broad and covers photographs of people where they are identifiable. If you plan to take photographs of your event for use in any material (such as your website or in brochures or newsletters), you should arrange notification forms for the people who appear in the images. These forms should explain the purpose of the photographs and how you plan to use them, in addition to the other notification requirements discussed in part 3 of this guide.
- While information about companies is not covered by Privacy Laws, it might be covered by confidentiality laws. For information on confidentiality- see our guide to intellectual property

What is sensitive information?

'Sensitive information' is a special category of personal information and is subject to stricter legal requirements for collection, storage, use and disclosure.

Under Privacy Laws, information is 'sensitive information' if it is or includes information or an opinion about a person's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual preferences or practices, or
- criminal record

Health information (discussed further below), genetic information and many aspects of biometric information are also 'sensitive' information' under the federal Privacy Laws.

Caution

Your organisation needs to distinguish between different types of personal information to make sure you deal with each type as required by law.

What is 'health information'?

'Health information' is generally afforded a higher level of protection under Privacy Laws.

'Health information' includes information or opinions about a person's:

- physical and mental health
- disability (at any time)
- health preferences (including future provision of health services)
- use of health services
- bodily donations (for example, blood, organs), and
- genetics

Example

Examples of 'health information' include:

- notes on a person's symptoms or diagnosis and treatment
- specialist reports or test results
- appointment and billing details
- dental records
- a person's healthcare identifier when it's collected to provide a health service
- prescriptions and other pharmaceutical purchases, and
- any other personal information (such as information about a person's sexuality, religion, date of birth, gender) collected to provide a health service

Other categories of confidential information

The following types of information are also protected. This guide does **not** cover these types of information.

- 'spent convictions' (old, minor criminal convictions)
- tax file numbers (extreme care must be taken with tax file numbers as special rules apply)
- electoral roll information
- surveillance information, and
- credit history

If you deal with this kind of information and are not aware of the particular privacy requirements that apply to your organisation, you should get a privacy lawyer's advice.

Caution

Strict legal requirements apply to the handling of information about a person's credit worthiness.

If your organisation deals with credit information, it should get advice on complying with these obligations.

Part 2

Is your organisation subject to Privacy Laws?

Is your organisation subject to Privacy Laws?

This part covers:

- the sources of Privacy Laws
- who Privacy Laws apply to

Once you have established that the information you collect, store, use or disclose may be considered 'personal', 'sensitive' or 'health' information, you need to work out which (if any) Privacy Laws apply to your organisation.

A not-for-profit organisation may be governed by one or more laws that make up the Privacy Laws.

Three separate sources of law make up the Privacy Laws:

1.	The Australian Privacy Principles (**APPs**) under federal Privacy Laws
2.	Applicable state and territory Privacy Laws (for example, government records and industry specific legislation)
3.	Applicable state and territory health privacy legislation (**Health Privacy Laws**)

Caution

Your organisation may have to comply with more than one set of privacy obligations listed above.

For example, an organisation that has a contract with a Victorian Government agency may need to comply with the APPs as well as the State Privacy Laws.

You will need to make sure your practices are consistent with all the Privacy Laws that apply to your organisation. If you're not sure, you should get legal advice.

The federal legislation is generally not intended to override state and territory privacy legislation but to operate alongside it.

Organisations that meet the criteria set out below must comply with Privacy Law obligations.

Federal Privacy Laws: Australian Privacy Principles (APPs)

The APPs are legal obligations under federal Privacy Laws. They apply to every Australian organisation and federal government agency that meets the qualifying criteria (set out below).

'Organisation' (defined in the Privacy Act) includes individuals, bodies corporate, partnerships, trusts and other unincorporated associations. 'Bodies corporate' includes many common legal structures in the not-for-profit sector, such as incorporated associations, co-operatives, companies limited by guarantee and indigenous corporations. Not-for-profit organisations that are unincorporated associations and trusts also fit into the definition of 'organisation'.

Criteria

Your organisation must comply with the APPs if it falls into any of the following categories:

- it has an annual turnover of more than $3 million in any financial year since 2002
- it provides a health service (which is broadly defined) to a person (even if the organisation's primary activity is not providing that health service)
- it trades in personal information (for example, buying or selling a mailing list)
- it is a contracted service provider under a Commonwealth contract (for example, an aged care provider or a disability services provider under a Commonwealth agreement)
- it is a credit reporting body
- it operates a residential tenancy database
- it is a reporting entity for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- it is an employee association registered or recognised under the *Fair Work (Registered Organisations) Act 2009* (Cth)
- it is a business that conducts protection action ballots
- it is a business prescribed by the *Privacy Regulation 2013*
- it is related to a body corporate (for example, a subsidiary) that meets any of the above criteria (even if your not-for-profit itself does not), or
- it has opted into the Privacy Act (choosing to comply, despite not meeting any of the above criteria)

The Office of the Australian Information Commissioner (**OAIC**) (an Australian Federal Government agency) has published a checklist can help you decide if your small business needs to comply with the Privacy Act

Note

Organisations that are not covered by the APPs can 'opt in' to be bound by the APPs. They are then treated as an 'organisation' for the purposes of the Privacy Act.

For more information on opting in and out see the Office of the Australian Information Commissioner (**OAIC**)'s website.

Examples of when the APPs apply

- ✓ You run a charity that recorded an annual income of $3 million in its most recent Annual Report. **The APPs apply to you.**
- ✓ You are a club with an annual turnover of less than $3 million, but your club has a program or facilities to assist members with injuries or improve fitness and health. It's probably providing a health service, especially if it hires a health professional. **The APPs apply to you.**
- ✓ You are a theatre company with an annual turnover of less than $3 million, but you enter into a sponsorship deal and, as part of that sponsorship deal, you pass your customer list to the sponsor corporation (ie. in exchange for the sponsorship benefit). **The APPs apply to you.**
- ✓ You are a not-for-profit organisation that provides childcare services or activities. While you have an annual turnover of less than $3 million per year, you collect, use and store information about children's allergies, disabilities and medical needs (ie. health information). **The APPs apply to you.**
- ✓ You are a subsidiary of a not-for-profit organisation and have an annual turnover of less than $3 million in Australia. Your not-for-profit organisation is part of a larger global network of not-for-profits. Your parent organisation (incorporated in the US under a different legal entity) has an annual turnover of over $3 million. You provide information about your members, donors or volunteers to your parent not-for-profit organisation. **The APPs apply to you.**
- ✓ You are a not-for-profit organisation that has an annual turnover of less than $3 million. You obtain funding from the Commonwealth Government to run a specific program and you enter into an associated funding contract. **The APPs apply to you.**

Example of when the APPs don't apply

- ✗ You are a sporting club that collects the names and addresses of team participants. You earn $120,000 in annual revenue. Provided you don't fall into any of the other categories listed above**, the APPs don't apply to you.**

Exemptions to the APPs

There are exemptions to the APPs.

Once you've considered whether your not-for-profit organisation is required to comply with the APPs under the 'threshold' criteria (set out above), you need to work out whether your organisation, or particular information it handles, falls into an exemption category.

The main exemption categories relevant to not-for-profit organisations are summarised below.

Employee records exemptions

If an employer handles information that is part of an employee record that is directly related to a person's current or former employment relationship, the employer's conduct is exempt from the APPs.

This exemption does not apply (and so the APPs may still apply) if the information is about:

- former job applicants (who were not employed)
- contractors
- volunteers, or
- employees of related entities (for example, subsidiaries)

Note – this exemption might not extend to records of an employee's (after-hours) behaviour on social media while employed by your organisation, or other records not related to the person's employment with your organisation.

Caution

Employee records that are exempt from the APPs may be subject to special requirements under the *Fair Work Act 2009* (Cth). If you are not sure about your obligations in handling employee records, you should get legal advice.

Note

Despite the employee records exemption under federal Privacy Laws, state and territory Privacy Laws may still apply to certain employee information.

In particular, the Health Privacy Laws may apply to private sector organisations, including to not-for-profits that handle health information (including employees' health information).

Example

You are contacted by a prospective employer of a former employee asking for personal information related to their employment record with your organisation. This information is subject to the employee records exemption.

However, during the course of the conversation, the prospective employer asks if you noticed any unusual activity on the employee's social media accounts during the course of their employment. It's unclear if this is covered by the APPs. Err on the side of caution when disclosing information regarding former employees – stick to what is in the employee's official record.

Government contractors' exemption

If an organisation is required to follow the APPs only because it has a contract with government, the organisation is only required to follow the APPs for personal information that it manages in relation to activities under that contract.

Example

Your not-for-profit organisation has an annual turnover of $1.2 million and is not normally bound by the APPs. Your group provides free after school care for refugee children, and also has a contract with the Federal Government to provide English language classes to adult migrants. The personal information you collect, use and disclose in relation to the government-funded English language program is protected by the APPs, but the personal information you manage for the privately-funded after school care program may be exempt.

If an organisation is required to do something under a government contract that is inconsistent with the APPs, an exemption applies so that the terms of the government contract can be met.

Example

You are a not-for-profit halfway house contracted by a state government to assist in rehabilitating juvenile offenders. You are required to disclose information regarding possible offences by residents under the terms of your contract, despite it conflicting with an APP. This information is subject to an exemption to the APPs and may be disclosed.

Political exemption

If you work on behalf of a registered political party or representative (with their authority), the work you do for them will be exempt from the APPs if the purpose of the work is connected with:

- an election
- a referendum
- the party or representative's participation in the political process, or
- facilitating acts or practices of the political party for the purposes of any of the above

Other exemptions

Other exemptions exist, but are not usually relevant to community organisations, for example:

- local councils or state or territory governments or authorities (these entities are exempt from the APPs and are usually subject instead to state and territory Privacy Laws)
- journalism exemption (this only applies when an organisation adopts other media privacy standards), and
- an exemption from some APPs for transfers of information between related organisations

Caution

If your organisation is required to comply with the APPs, and you're not sure whether the information you deal with might fall into one of the exempted categories discussed here, you should get legal advice.

State and territory Privacy Laws and Principles

Australian state and territory information privacy principles (**IPPs**) apply to their respective government agencies (including public sector agencies, local councils, courts, state police, etc.) except where the Health Privacy laws apply. The state and territory IPPs may also apply to organisations that contract with the relevant state or territory government.

State and territory IPPs	
ACT	*Information Privacy Act 2014* (ACT) sets out 13 Territory Privacy Principles in Schedule 1
NSW	*Privacy and Personal Information Protection Act 1998* (NSW) sets out 12 Information Protection Principles (New South Wales IPPs) in Part 2, Division 1
NT	*Information Act 2002* (NT) sets out 10 Information Privacy Principles in Schedule 2
Qld	*Information Privacy Act 2009* (QLD) sets out 11 Information Privacy Principles in Schedule 3
SA	Part II of the administrative instruction, PC012 – Information Privacy Principles Instruction provides a set of Information Privacy Principles
Tas	*Personal Information Protection Act 2004* (Tas) sets out 10 Personal Information Protection Principles in Schedule 1
Vic	*Privacy and Data Protection Act 2014* (Vic) sets out 10 Information Privacy Principles in Schedule 1
WA	There is currently no legislative privacy scheme, however the *Privacy and Responsible Information Sharing Bill 2024* (which would establish information privacy principles for public sector agencies) is currently before the WA Assembly. In addition, some privacy principles (dealing with access to information and correction of information) are covered by the *Freedom of Information Act 1992* (WA)

Health Privacy Laws

New South Wales, Victoria and the Australian Capital Territory each have their own specific Health Privacy Laws. The Health Privacy Laws apply a higher standard of protection to certain health information.

The state and territory Health Privacy Laws are set out in the following legislation:	
ACT	*Health Records (Privacy and Access) Act 1997* (ACT)
NSW	*Health Records and Information Privacy Act 2002* (NSW)
Vic	*Health Records Act 2001* (Vic)

Your organisation may be required to comply with Health Privacy Laws (in addition to federal Privacy Law) if you operate in New South Wales, Victoria or the Australian Capital Territory and:

- you are a health service provider, or
- you collect, hold or use health information (described in part 1 of this guide)

Health service providers

A health service provider may be a public or private organisation including:

- traditional health service providers (such as public or private hospitals, day surgeries, medical practitioners, pharmacists and allied health professionals)
- complementary therapists (such as naturopaths and chiropractors)
- gyms and weight loss clinics, and
- childcare centres and private schools

If you think your organisation may collect, hold or use health information, we recommend you get legal advice to understand your organisation's obligations.

Examples of when Health Privacy Laws apply

✓ You are a contracted health service provider to Victoria's 12 publicly managed prisons. You are required to comply with the applicable Health Privacy Laws.

✓ You run a safe injection house that takes the names of drop-in patients. You may be required to comply with the applicable Health Privacy Laws

Example of when Health Privacy Laws don't apply

✗ You provide first aid at music festivals on an anonymous basis. You would not be required to comply with the Health Privacy Laws.

Part 3

What are your organisation’s obligations under Privacy Laws?

What are your organisation's obligations under Privacy Laws?

This part covers:

- the Australian Privacy Principles (**APPs**) under federal Privacy Laws
- requirements for your privacy policy
- rules for collecting and storing information
- when you may use or disclose information (including direct marketing)
- access to and correcting information
- responding to privacy breaches and requirements to report breaches
- what happens if you don't comply with Privacy Laws
- ongoing obligations, and
- the differences between state and territory Privacy Principles (**IPPs**)

If your organisation holds or wants to collect 'personal', 'sensitive' or 'health' information about a person and Privacy Laws apply to your organisation, you need to know what your organisation must do to meet its legal obligations.

The Australian Privacy Principles (**APPs**), mentioned in part 2 above, are 13 legally binding principles which set the basic standard for protecting 'personal', 'sensitive' and 'health' information at the federal level.

The APPs set out requirements about how organisations may collect, use, disclose and store these types of information.

The APPs are also considered best practice for privacy, so even if your not-for-profit organisation is not legally bound by the APPs, it's a good idea to follow them. State and territory Privacy Laws largely replicate the APPs, but there are some differences (summarised at the end of this section).

The APPs cover the following subjects (explained further below).

APP	Subject
APP 1	Open and transparent management of personal information
APP 2	Anonymity and pseudonymity
APP 3	Collection of solicited personal information
APP 4	Dealing with unsolicited personal information
APP 5	Notification of the collection of personal information
APP 6	Use or disclosure of personal information

APP 7	**Direct marketing**
APP 8	**Cross-border disclosure of personal information**
APP 9	**Adoption, use or disclosure of government related identifiers**
APP 10	**Quality of personal information**
APP 11	**Security of personal information**
APP 12	**Access to personal information**
APP 13	**Correction of personal information**

Your organisation's privacy policy

If APPs apply to your organisation, you must have a clearly-expressed and up-to-date privacy policy.

Your privacy policy must cover a number of things (listed below).

You must also make the policy as available as is practically possible (for example, on your website) and, if anyone asks for the policy, you must give them a copy of it (for example, by posting it to them) (**APP 1**).

It's good practice to have a copy of your privacy policy accessible either in full or as a link in the footer section of all pages on your website so it is readily available.

Things to include in your organisation's privacy policy:	
• the kind of personal information you collect and hold	☐
• how you collect and hold that personal information	☐
• the purposes for which you collect, hold, use or disclose that personal information	☐
• how someone may access and correct the personal information you hold about them	☐
• how someone can complain about a suspected breach of privacy laws	☐
• whether you are likely to disclose the information to overseas recipients	☐
• if you are disclosing information to people overseas, the countries where those people might be (if it's practical to specify)	☐
• an explanation of the right to anonymity and pseudonymity	☐
• whether you use personal information for direct marketing	☐

Tips for privacy policies

- **Don't copy text from another organisation's policies, because that text might:**
  - not be relevant to your organisation's handling practices
  - be drafted according to laws from states or countries different from those that apply to you
  - contain details specific to an external organisation
  - not cover all the requirements you're obliged to meet, or
  - be protected by copyright
- **Don't over-commit.** An example of promising too much could be: 'we will never disclose your information without your consent'. Failing to comply with your privacy policy can have serious consequences – overcommitting can make it difficult to avoid breaking that commitment
- **Keep it easy to read.** Draft your privacy policy in plain and simple language to help people understand the policy and avoid potential legal ambiguity
- **Include relevant detail.** Making your policy easy to consume doesn't mean that it shouldn't contain all the information users need to know
- **Keep it updated.** The ways your organisation collects and uses personal information can change, and so do technology and laws. Review your privacy policy regularly to make sure it reflects your current practices and obligations.
- **Keep it easy to access.** The best place for your privacy policy is on your website, with a clearly visible link and an easily downloadable resource. It's also a good idea to keep a hard copy in your office.

Rules for collecting information

Collecting personal information

Things to include in your organisation's privacy policy:

- only collect personal information reasonably necessary for your organisation's functions or activities (**APP 3**)
- only collect personal information by 'lawful and fair means'– that is, not through criminal or illegal activity, trickery or deception (**APP 3**)
- only collect personal information directly from the person it belongs to, unless it's impossible or not practical to do this (**APP 3**)
- give individuals the option of remaining anonymous or using a pseudonym, unless this is not practical, or your organisation is required by law to deal with an identified person (**APP 2**)
- tell individuals what your organisation will use their personal information for (**APP 5**)
- tell individuals if you collect personal information for the purpose of direct marketing (**APP 7**)

Tip

If you use street-based direct marketing, you may only collect personal information by lawful or fair means. You can't trick someone into telling you where they live, or how much they earn – keep your questions straight and to the point! Make sure your street representatives know their obligations regarding what information they are to collect and how they are to collect it.

Collecting sensitive and health information

When collecting sensitive information and health information, your organisation must get the person's consent, unless an exception applies. Consent is discussed below.

You must not collect sensitive or health information unless:

- the person specifically consents to the information being collected, and
- the information is reasonably necessary for your organisation's functions or activities

Exceptions for 'Permitted Situations' and 'Non-profit organisations'

However, sensitive information can be collected, used, or disclosed without consent in 'permitted situations'. These are listed in the Permitted Situations section of this guide.

In addition, organisations that meet the federal Privacy Law definition of a 'non-profit organisation' may collect certain types of sensitive information without consent.

'Non-profit organisation' is defined as a not-for-profit organisation 'that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes'. If your not-for-profit organisation fits this definition, you may collect 'sensitive' information without consent if:

- the information relates to your organisation's activities, and
- the information relates solely to the members of the organisation, or to people who have regular contact with the organisation in connection with its activities

Examples

Circumstances where not-for-profit organisations may be entitled to collect sensitive information without consent include the following:

- a religious not-for-profit organisation collecting information about their member's views on religious or moral issues
- a trade union collecting information about a job applicant's political views, or
- a community not-for-profit organisation that assists people with disabilities collecting information about their disability, as well as diagnosis and medical reports in order to provide counselling and support only. (This exception would not apply if the organisation is providing any kind of health service).

Caution

- An organisation conducting activities for another purpose not related to its core purpose can't rely on this exception.
- A not-for-profit organisation can rely on the exception if there is a clear relationship between the information collected and the activity. For example, the information may relate to a fundraising activity by a not-for-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose.
- Collection of sensitive information about a relative of the member would not be covered, unless that person also had regular contact with the not-for-profit organisation.

Best practice

Regardless of whether consent is required for the collection of sensitive information, you should apply the general rules for collecting personal information. That is:

- only collect information reasonably necessary for your organisation's functions or activities
- collect the information by lawful and fair means
- try to collect the information directly from the person concerned
- ensure that the only persons who have access to the information in your organisation are those who require access to it, and
- tell the person the identity of your organisation and the purpose of collecting the information, as well as the other notification matters listed under 'Things you are obliged to tell the person providing information' section of this guide

Collection from third parties

If you can't reasonably and practically collect health information from individuals themselves, you can collect it from a third party in very limited circumstances. This might include:

- in an emergency where background health information is collected from relatives, or
- where a person is referred to a medical specialist and the specialist seeks relevant information from a referring provider

Regardless of whether you collect the information directly from the person or from a third party, Privacy Laws require that you notify the person that you collected the information. However, Privacy Laws recognise it might not be reasonably practical to notify the person in some instances. For example, in an emergency situation, there may not be enough time to notify the person concerned.

Tip

Health information has a number of special protocols that must be followed, and state or territory laws may apply in addition to the federal Privacy Laws. If you manage health information, make sure you know your organisation's obligations.

Things you are obliged to tell the person providing information

When you collect personal information (or as soon as you reasonably can after collection), you must take steps to make sure you make the person aware of certain mandatory information (APP 5):

- your organisation's identity and contact details
- if you collected the information from a third party or the person is otherwise unaware of the collection of their personal information, the fact that your organisation has collected the personal information
- if the collection of personal information is required or authorised by law or a court or tribunal order, the fact that it's so required or authorised (including the name of the law or details about the court or tribunal order)
- the purposes for which the information is being collected
- the main consequences if the personal information is not collected
- any other person or entity to which you may disclose the personal information
- circumstances under which your organisation would disclose the information or be required to disclose the information
- that your privacy policy has information about how the person may access and correct the information you hold about them, or otherwise seek correction of the information
- that your privacy policy has information about how someone can make a complaint about a breach of the applicable APPs, and
- whether you are likely to disclose personal information to overseas recipients and, if so, the countries in which those recipients are located (if it's reasonably practical to specify the locations)

Note

The process for a user to remove their information from your service should be easy and accessible.

You should also make the potential consequences of the user withdrawing their consent clear – for instance:

- your organisation may not be able to rely on past consent in relation to its services, or
- the user may no longer have access to your services

You can make the person aware of this information in a number of ways.

Typically, organisations give the person a short privacy notice (sometimes called a 'collection notice') which addresses the matters listed above.

You could also provide, or refer the person to, your privacy policy. If you do this, make sure your privacy policy covers the matters listed above in relation to the particular collection of personal information.

Getting consent

Although it's not always practical to get a person's consent (nor necessary when collecting non-sensitive personal information), if you get consent, your organisation will generally be allowed to deal with that information under the Privacy Laws in any way that is consistent with the consent provided.

Note

Consent is required to collect sensitive information and health information, unless an exception applies (**APP 3**).

There are strict requirements about the type of consent that must be given. For instance, consent, whether express or implied, must involve the person:

- being adequately informed before giving consent
- giving consent voluntarily
- giving consent that is current and specific, and
- having the capacity to understand and communicate their consent

Consent doesn't have to be in writing, but it's a good idea to keep a record of a person's consent in case it's challenged later.

Consent can take a variety of forms. Where practical, a signature or check box is a good way to document evidence of consent. Voice recordings are also often used when consent is sought over the phone.

Consent can be express or implied, but privacy regulators:

- caution against inferring consent from a person's failure to opt out, and
- require that consent be fully informed and provided voluntarily

It's therefore important to give users the opportunity to opt out to communications (such as communications by email or text).

Tips

- Use a 'double opt-in' to give the user another opportunity to document evidence of consent. For example, if you request a person's name and email address, you can require them to confirm their opt-in to the mailing list by clicking on a link in a confirmation email (which can be auto-generated) you send to them.
- Make sure you provide existing users with details of updates to your privacy policy when you amend your policy.

Continuing consent

Evidence of continuing consent is important in many circumstances.

Just because you obtained consent for one or more matters doesn't mean the user has provided consent to process, store or handle their data in other ways.

Your services, the law or prevailing circumstances may change, and it may be important at different times to seek and affirm consent that is both current and specific.

Caution – consent and capacity

Always consider whether someone has capacity to give you their consent.

- Are they under 18?
- Do they appear to understand what they are consenting to?
- Could they be suffering from an illness (such as dementia) that prevents them from providing informed consent?
- Is the person temporarily incapacitated?
- Can the person sufficiently comprehend the language or technological methods through which you are trying to engage?

You may need to involve a guardian, or someone recognised as a 'responsible person' in the consent decision. In these and other circumstances, it may be prudent to offer the individual support services, such as an interpreter.

Make sure the person you are engaging, or their parent or guardian:

- understands what they are consenting to, and
- can and does communicate their decision on consent

For more information, see the Office of the Australian Information Commissioner's (OAIC) webpage 'Consent to the handling of personal information'.

Unsolicited information

Unsolicited information (**APP 4**) is personal, sensitive or health information that you have received that you took no active steps to collect. If you receive unsolicited personal information, you need to consider whether you could have lawfully collected the information. That is:

- was the information reasonably necessary for one or more or your organisation's functions or activities? and
- was it sensitive information requiring consent?

If you could have lawfully collected the information, you may keep the information, but you must handle it in accordance with Privacy Laws. This includes notifying the person concerned where reasonable.

If the information is not reasonably necessary for one or more of your organisation's functions or activities, then you must destroy or de-identify the information. However, before you destroy information, you must make sure you don't have a legal requirement to retain it. If you are not sure, get legal advice before destroying or de-identifying information.

Different rules apply to information in Commonwealth records. A Commonwealth record includes any record that is, or that has been deemed by law to be, a record that is the property of the Commonwealth. Commonwealth records must not be destroyed as they must be handled in accordance with the *Archives Act 1983* (Cth).

Example

A person sends their CV to your organisation, requesting a job (but not responding to an advertised vacancy). There are no positions currently available, but the person has a relevant skillset and could be a potential candidate for future positions. Your organisation can keep that information on file, as long as you give the person the required notification under APP 5 and handle the information in accordance with the Privacy Laws.

Storing personal information

Your organisation must take reasonable steps to protect the personal, sensitive and health information it stores from misuse, interference and loss, and from unauthorised access, modification or disclosure (**APP 11**).

Security measures

Depending on your organisation's circumstances, consider the following security measures:

- require staff to lock relevant documents away
- place access restrictions on relevant documents or systems, including electronic access restrictions (the more people who have access, the greater likelihood a breach may occur)
- enforce a 'clean desk' policy to minimise the risk of inadvertent disclosure of personal information
- place computer screens out of the view of others, particularly visitors to the organisation
- limit the use of portable storage devices, including laptops, disks and USB keys, or use encryption or other security measures
- record audit trails of access to documents
- encrypt documents containing personal information, particularly when those documents are being sent by email
- to the extent feasible, present data in a way that individuals can't be identified or linked to the data in the case of a breach
- include email addresses for group emails in the 'BCC' field rather than the 'to' field so recipients can't see other recipients' email addresses
- include confidentiality and privacy clauses in agreements with volunteers or others who have access to the personal information (and give specific examples of activities that would be considered a breach), and
- make sure employees, volunteers or others return information at the end of their employment or involvement with the organisation and that they have no method of retaining access to information

Caution – cloud-based storage

In addition to taking the security measures listed above, if you use internet (or 'cloud') based storage systems for your data, there are other important issues to consider.

Under the APPs, if you outsource data services to a third-party provider based overseas (such as a server provider in another country), you must take reasonable steps to make sure that the third-party provider does not breach the APPs.

Also, if that provider breaches the Privacy Act, you may be accountable for those breaches!

Cloud storage contract checklist

Steps you can take to limit the possibility of your third-party provider breaching the APPs include:	
• in any contract you sign with an overseas service provider, require the provider to comply with the APPs, your privacy policy and include indemnities against any breach of the applicable Privacy Law or Health Privacy Law	☐
• provide the service provider with a copy of your privacy policy	☐
• understand how the third-party provider handles, stores, and deals with data and personal information	☐
• ensure that by providing access to the data that your organisation's or the third-party provider's processes are not rendering the data more publicly accessible (this is how some of the most well-publicised data breaches have occurred)	☐
• maintain strong access, security controls and procedures over who has access to your data and what they can do with it	☐

For more information about how to store personal information securely, read the OAIC guide to securing personal information.

Other recommended action

Your organisation must also take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date and complete. It must also be relevant to the purposes for which it's being used or disclosed (**APP 10**).

If your organisation is storing personal information it no longer needs, it must take reasonable steps to destroy or de-identify the information, unless:

- the information is contained in a Commonwealth record, or
- there is a legal requirement to retain the information

Health information

If your organisation 'holds' health information, you may have additional obligations under the APPs and state and territory Health Privacy Laws (which only apply in NSW, Vic and the ACT) or other state and territory Privacy Laws applicable to your not-for-profit.

You will hold health information if you possess a document (paper or electronic), or if your organisation has control over a document, that contains health information.

If you participate in the My Health Record system, you must comply with the *My Health Records Act 2012* (Cth) (***MHR Act***) and the *Healthcare Identifiers Act 2010* (Cth) (***HI Act***). The *MHR Act* limits when and how health information included in a person's My Health Record can be collected, used and disclosed.

If you are storing health information, you have certain obligations to the person whose information you have.

You are required to ensure, at their request, that that person has:

- an understanding of:
  - why you are storing that information

  - how you collected that information
  - details of the health information you have
  - what rights they have to access that information, and
- an ability to update, correct, or amend that information (subject to a reasonable request)

Tip

Regardless whether a document is located in your organisation or your state or territory, or whether you have sole custody of the information, if the information has a connection to your organisation's state or territory operations, a state or service contract, or a client of your state or territory, the state or territory privacy requirements may apply.

Using or disclosing information

Using information for the primary purpose

Unless an exception applies, you must not use or disclose personal information you have collected for any other reason other than the **primary purpose** you collected it for (**APP 6**). The exceptions are listed below.

Tip

Remind staff regularly of your organisation's primary purpose for collecting personal information.

Consider including a 'mission statement' or 'primary objective' reminder on documents circulated to telemarketers or street side information collectors.

Using information for a secondary purpose (exceptions)

A secondary purpose is any purpose other than the primary purpose for which you collected the information. These are

- **Consent.** The person specifically consents to its use for another purpose.
- **Reasonable expectation.** This exception is a two-limb test. First, the person must reasonably expect that you would use or disclose their information for such a purpose. Second, the secondary purpose must be related to the primary purpose, that is, it must be connected or associated with the primary purpose. If the information is sensitive information, then the secondary purpose must be directly related to the primary purpose, that is, it must be closely associated with the primary purpose.
- **Law.** An exception in the law (either in Privacy Laws or in another law) expressly applies to permit the secondary use of the information. For an overview of some exceptions in law, see the Permitted Situations Quick Reference Guide in this guide.

Example

Your not-for-profit collects personal information from people interested in receiving news about saving the rainforest, and you notify them you are collecting their personal information to provide email updates. You must not use that information to do anything other than this unless you get the person's specific consent (or an exception applies).

Additional requirements limit the adoption, use and disclosure of government identifiers (for example, Medicare number, drivers licence number, passport number).

Direct marketing

Direct marketing (**APP 7**) is communicating with a person to promote goods and services and can include fundraising. Any contact information should be secured through an 'opt-in' system. If your organisation uses or discloses personal information for the purposes of direct marketing, you should consider the following issues.

You can only use or disclose sensitive information (including health information) for direct marketing if a person has consented to that use or disclosure. You can only use or disclose non-sensitive personal information for direct marketing if you meet all of the following conditions:

- you collected that information **directly from the person**
- the person whose information is disclosed would **reasonably** expect you to use the information for direct marketing
- you provide an easy '**opt-out**' option for anyone who doesn't want to receive direct marketing, and
- the person has not chosen to opt out

You may also use or disclose non-sensitive personal information for the purpose of direct marketing in circumstances where you collected the personal information from a third party, or the person would not expect you to use or disclose their personal information for the purpose of direct marketing, if you meet all of the following conditions:

- you have the person's consent or it's not practical to obtain consent
- you provide a simple opt-out mechanism from direct marketing and, in each direct marketing communication, you include a prominent statement drawing attention to this mechanism, and
- the person has not chosen to opt out

Caution – the Spam Act

In addition to the Privacy Laws, the *Spam Act 2003* (Cth) (**Spam Act**) prohibits the sending of unsolicited commercial electronic messages (spam) with an Australian link. A message has an Australian link if it originates or was commissioned in Australia or originates overseas but was sent to an address accessed in Australia.

Where the Spam Act or the *Do Not Call Register Act* 2006 (Cth) apply, they prevail over the requirements of APP 7 in relation to the relevant act or practice.

Not-for-profit organisations, community service organisations and non-government organisations must comply with the Spam Act. However, in some circumstances under the Spam Act, charities registered with the Australian Charities and Not-for-profits Commission may be exempt from obtaining consent from recipients.

Access to and correcting personal information

Accessing personal information (APP 12)

If a person asks for access to their own personal information held by your organisation, you are generally required to give access in the way the person has requested. You should respond to the request in a reasonable period. Take care, when providing access to information, that you don't inadvertently disclose a third party's personal information.

Your organisation may refuse a request for access in limited circumstances (for example, where providing access would result in a serious threat to a person's safety or where the access would be unlawful). If your organisation refuses to give access, you must provide the person with a written notice setting out the reasons for the refusal and the mechanism for making a complaint about it.

Your organisation can't charge the individual for the making of the request. Your organisation can, however, charge the individual for giving access to the personal information but the charge must not be excessive.

Correcting personal information (APP 13)

If a person can show that personal information about them held by an organisation is inaccurate, incomplete, irrelevant, out-of-date or misleading, the organisation must:

- take reasonable steps to correct the information and notify third parties to which it has provided the information, or
- if the information is not correct, provide the person with written reasons for the organisation's refusal to correct the information, including information about how to make a complaint and a statement noting the person claims the information is incorrect, incomplete, irrelevant, out-of-date or misleading

Your organisation must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

Disclosing across borders

Because more organisations operate across national borders than ever before, privacy has become an international problem. Many not-for-profits are not sure what privacy obligations apply to information they receive from overseas, as well as information they send or store overseas.

Under federal Privacy Laws, before an organisation discloses personal information to an overseas recipient, it must take reasonable steps to ensure the overseas recipient does not breach the APPs (**APP 8**). This requirement does not apply if the disclosing organisation reasonably believes that:

- the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially similar to protection given under the APPs, and
- there are mechanisms available to enforce that protection

Tip

It's always good practice to identify the location of the countries in which the organisation is likely to disclose to if it is practicable to do so.

For more information on cross-border disclosures, see OAIC's guide to Cross-border disclosure of personal information - Chapter 8: APP 8.

Responding to a privacy breach

The Office of the Australian Information Commissioner (OAIC) provides guidance on responding to a privacy breach in its guide to Data breach preparation and response.

This guide sets out a four-step process for an organisation to follow when a breach of privacy occurs. A summary of the steps is below. Steps 1, 2 and 3 can be taken at the same time.

Step 1 Contain	• Take action to stop the breach happening further • Take care not to destroy evidence that could help you work out how the breach happened
Step 2 Assess	• Work out what happened and assess risks to people • If possible, take action to stop or mitigate any risks • Assess whether there has been a notifiable data breach (see below) • This assessment should be made within 30 days following the breach
Step 3 Notify	• If required, following the assessment, notify the people affected and the regulator (OAIC) of the breach
Step 4 Review	• Review the breach circumstances • Identify action to take to prevent breaches in future and take this action

When must you report a breach?

All entities subject to federal Privacy Laws must comply with the notifiable data breaches scheme set out in the Privacy Act (**NDB Scheme**). Under the NDB Scheme, if an actual or suspected date breach that is likely to result in serious harm occurs, you must notify the regulator and people whose personal information is involved.

Has a notifiable data breach occurred?

Key questions to ask in assessing whether a notifiable data breach has occurred include:

Key questions to ask in assessing whether a notifiable data breach has occurred include:
1. Is your organisation subject to federal Privacy Laws? For information to answer this question, see part 2 of this guide. Only entities subject to federal Privacy Laws are required to comply with the NDB Scheme.
2. Does the breach or potential breach involve personal information? For an outline of what personal information includes, see part 1 of this guide. Only breaches involving personal information are subject to the NDB Scheme.
3. Has there been unauthorised access to, disclosure or loss of personal information? Unauthorised access may refer to circumstances where a person has accessed data without permission. This includes circumstances where an employee (or non-employee) accesses a work computer with sensitive information, or where your organisation has been hacked or subject to a malware threat. Unauthorised disclosure may also refer to circumstances where a person discloses information to another person who does not have authority to access the information (for example, if an employee sources personal information such as an address and discloses the information to another person).

Unauthorised disclosure can also refer to circumstances where information was accidentally leaked or disclosed – for instance if all or part of a file or database that is restricted is made publicly accessible online.

Loss can refer to circumstances where you can't retrieve the lost file or information (for example, if an employee loses a work computer or USB on a train).

4. **Is the unauthorised access, disclosure or loss likely to cause serious harm to any person who the information is about?**

   Serious harm can be psychological, physical, financial, emotional or reputational.

   The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible).

   You should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm.

If you answer 'yes' to any of these questions, and you are unable to prevent the likely serious harm with remedial action, it is likely that a notifiable data breach has occurred, and you will need to make mandatory notifications.

Making mandatory notifications

You must make notifications under the NDB Scheme to the OAIC and affected people (ie. any person who the compromised personal information is about and people at risk of harm from the breach) in accordance with the Privacy Act requirements. The notification (to both the OAIC and affected people) must include a description of the breach and recommended steps for affected people.

Where it's not practical to notify each affected person personally (for example, where you don't have contact details for each person), you should publish notifications on your organisation's website and take reasonable steps to publicise the information.

The notification to the OAIC may be made through the OAIC's Notifiable Data Breach Form.

Managing actual and suspected breaches

Organisations must assess a suspected data breach promptly (and must, if required, generally report a notifiable data breach within 30 days). The OAIC recommends that all organisations have a plan in place to deal with actual or suspected data breaches. A plan should help you minimise the harm of any breach and make an efficient assessment of whether mandatory notification is required.

For more information on preparing for and responding to breaches, see the OAIC's guide to data breach preparation and response.

What happens if your organisation doesn't comply with Privacy Laws?

Failing to comply with your privacy obligations can have serious consequences, both legally and for the reputation of your organisation.

The OAIC has the power to seek court enforced fines up to 2,000 penalty units at $275 per unit against an organisation for serious or repeated interferences with a person's privacy (subject to indexation).

The maximum penalty for a body corporate for serious and repeated interferences of privacy is the greater of:

- AUD 50,000,000

- if a court can determine the value of the benefit obtained from the contravention – three times the value of the benefit, or
- if a court cannot determine the value of the benefit obtained from the contravention – 30% of the body corporate's adjusted turnover during the breach turnover period

The Privacy Commissioner also has a range of other powers, including powers to:

- make a determination that your organisation contravened the Privacy Act, and
- conduct privacy assessments (previously called audits)

These determinations and assessment findings are publicly available on the OAIC's website, so can cause reputational harm.

Damages include economic loss to restore a person to the same position they would have been in if they had not been wronged. It also includes non-economic loss for when a person is found to have faced certain hardships due to relevant circumstances such as pain, suffering, disability as well as loss of amenity of life, past and future. As at September 2024 the maximum amount awardable for non-economic loss in NSW is $350,000.

Ongoing obligations

Not-for-profit organisations have an ongoing obligation to make sure they continue to comply with Privacy Laws.

The OAIC has published a privacy management framework with four steps that not-for-profits and other organisations should take to ensure compliance.

Four steps to ensure compliance:

Step 1.	Embed a culture of privacy that enables compliance
Step 2.	Establish a robust and effective privacy process
Step 3.	Evaluate your privacy processes to ensure continued effectiveness
Step 4.	Enhance your response to privacy issues

How your organisation implements these steps will depend on a number of factors, including the size of your organisation, your system of governance, and the information that you are dealing with.

Comparison of Commonwealth and State and Territory Privacy Principles

The table below provides a high-level comparison of some of the key privacy principles. It's intended as reference guide only and is not a substitute for legal advice or for reading the privacy principles.

Commonwealth	States and Territories	
APP 1 – Open and transparent management of personal information		
APP 1.1 – Organisation must be open and transparent in its management of personal information	ACT NSW NT QLD SA TAS VIC WA	TPP 1.1 IPP 6 IPP 5 IPP 5, 2(3) - PIPP 5 IPP 5 -
APP 2 – Anonymity and pseudonymity		
APP 2.2 – Individuals must have the option of not identifying themselves, or of using a pseudonym (where lawful and applicable)	ACT NSW NT QLD SA TAS VIC WA	TPP 2.1 - IPP 8.1 - - PIPP 8 IPP 8 -
APP 3 and APP 4 – Collection of personal information		
APP 3.1 and 3.2 – Information must be reasonably necessary for or directly related to your organisation's functions or activities	ACT NSW NT QLD SA TAS VIC WA	TPP 3.1 IPP 8(1) IPP 1.1 IPP 1(b) - PIPP 1(1) IPP 1.1 -
APP 3.3 and 3.4 – Additional requirements in relation to 'sensitive information'	ACT NSW NT QLD SA TAS VIC WA	TPP 3.3 IPP 19(1) IPP 10 - - PIPP 10 IPP 10 -
APP 3.5 – Must only collect by lawful and fair means	ACT NSW NT QLD SA TAS VIC	TPP 3.5 IPP 8(2) IPP 1.2 IPP 1(2) IPP 1 PIPP 1(2) IPP 1.2

	WA	-
APP 3.6 – Information must be collected directly from the person unless exceptions apply	ACT NSW NT QLD SA TAS VIC WA	TPP 3.6 IPP 9 IPP 1.4 - - PIPP 1(4) IPP 1.4 -
APP 5 – Notification of the collection of personal information		
APP 5.1 – Organisation must take steps (if any) that are reasonable in the circumstances to notify/ensure that the individual is aware of certain matters	ACT NSW NT QLD SA TAS VIC WA	TPP 5.1 IPP 10 IPP 1.3, 1.5 IPP 2(3) IPP 2 PIPP 1(3) IPP 1.3 -
APP 6 – Use or disclosure of personal information		
APP 6.1 and 6.2 – Organisation must only use or disclose personal information for the primary purpose for which it was collected unless an exception applies	ACT NSW NT QLD SA TAS VIC WA	TPP 6.1, 6.2 IPP 17 and 18 IPP 2.1 IPP 9,10, 11 IPP 8, 10 PIPP 2 IPP 2.1, 2.2 -
APP 7 – Direct marketing		
APP 7.1 – An organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.	ACT NSW NT QLD SA TAS VIC WA	TPP 7 (s 23) - - IPP 11(4) - - - -
APP 8 – Cross-broader disclosure of personal information		
APP 8.1 – Restrictions on cross border disclosure of personal information	ACT NSW NT QLD SA TAS VIC WA	TPP 8.1 - IPP 9.1 - - PIPP 9 IPP 9.1 -
APP 9 – Adoption, use or disclosure of government related identifiers		

APP 9.1 – Restrictions on organisations adopting a government related identifier of an individual as its own	ACT NSW NT QLD SA TAS VIC WA	TPP 9 - IPP 7.2 - - PIPP 7(2) IPP 7.2 -
APP 9.2 – Restrictions on organisations using or disclosing a government related identifier of an individual	ACT NSW NT QLD SA TAS VIC WA	TPP 9 - IPP 7.3 - - PIPP 7(3) IPP 7.3 -
APP 10 – Quality of personal information		
APP 10.1 – Must take reasonable steps (if any) to ensure that the personal information it collects is accurate, up to date and complete	ACT NSW NT QLD SA TAS VIC WA	TPP 10.1 IPP 114(a) IPP 3.1 IPP 7 IPP 3 PIPP 3 IPP 3 -
APP 10.2 – Must take reasonable steps (if any) to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant	ACT NSW NT QLD SA TAS VIC WA	TPP 10.2 IPP 16 IPP 3.1 IPP 8 IPP 9 PIPP 3 IPP 3 -
APP 11 – Security of personal information		
APP 11.1 Organisation must take reasonable steps to protect information it holds from misuse, interference and loss and unauthorised access, modification or disclosure	ACT NSW NT QLD SA TAS VIC WA	TPP 11.1 IPP 12 IPP 4.1 IPP 4 IPP 4 PIPP 4(1) IPP 4 -
APP 11.2 – If an organisation no longer requires personal information, it must take reasonable steps to destroy or de-identify the information (subject to any document retention laws)	ACT NSW NT QLD SA TAS VIC WA	TPP 11.2 IPP 12 IPP 4.2 - - PIPP 4(2) IPP 4.2 -

APP 12 – Access to personal information		
APP 12.1 An organisation must on request by the individual, give the individual access to the information, subject to some exceptions	ACT NSW NT QLD SA TAS VIC WA	TPP 12.1 IPP 14 IPP 6.1 IPP 6 IPP 5 PIPP 6(1) IPP 6.1 -
APP 13 – Correction of personal information		
APP 13.1 – If an organisation is satisfied that information it holds is inaccurate, out-of-date, incomplete, irrelevant or misleading, or the individual requests the entity to correct the information, the entity must take reasonable steps correct the information.	ACT NSW NT QLD SA TAS VIC WA	TPP 13.1 IPP 15 IPP 6.3, 6.4 IPP 7(1) IPP 6 PIPP 6(2) IPP 6.5 -

Part 4

Fundraising and privacy

Fundraising and privacy

This part covers

- privacy issues when fundraising, and
- special considerations for private ancillary funds

Privacy issues when fundraising

If your organisation is subject to federal Privacy Laws and is collecting, using, storing or disclosing personal information as part of, or in connection with, its fundraising activities, you will need to make sure your activities comply with the Privacy Laws. You must:

- notify donors, volunteers, clients and others that you intend to use the personal information you collect from them for fundraising purposes from the start
- If you share your donor lists with other organisations, make sure that you explain who their information might be passed to
- always offer donors who support fundraising campaigns a choice about receiving information on non-fundraising activities or new campaigns from the start, and
- provide a prominent, simple opt out option in all fundraising communications

If you haven't notified a person that their personal information might be used for fundraising purposes, don't use it for those purposes unless:

- you first obtain consent, or
- an exception applies (for example, for non-sensitive personal information, the fundraising purpose is related to the primary purpose and the person would reasonably expect you to use the information in that way)

Note

Always consider the capacity of children, young adults, or people with compromised capacity when obtaining consent.

Tip

It's a good idea to only allow staff access to client information on a 'need to know' basis. For example, make sure that people involved in getting donor memberships don't have routine access to personal information that may be kept on client databases, and put checks and balances in place to protect the security of personal information.

For information about the fundraising laws that apply in each state and territory see our fundraising resources

Private ancillary funds

Details of charities registered with the Australian Charities and Not-for-profits Commission (**ACNC**) can be viewed by the public on the ACNC Register. Registration with the ACNC is a prerequisite for a charity to access certain Commonwealth tax benefits. For this reason, although charity registration is voluntary, most not-for-profits that are charitable organisations register with the ACNC.

Charities that are private ancillary funds may reveal the personal information of individual donors on the ACNC Register. An ancillary fund is a fund that links donors with an organisation that has deductible gift recipient status. If your organisation is a private ancillary fund and you are concerned that publication of a donor name, ABN, contact details, governing rules, financial reports or annual information statement is likely to result in the identification of the donor, you can apply to have identifying information withheld under the *Australian Charities and Not-for-profits Commission Regulation 2013* (Cth) before registration.

If your not-for-profit is a private ancillary fund and a charity that was endorsed by the Australian Taxation Office (**ATO**) for charity tax concessions before December 2012, it will be automatically registered with the ACNC.

Part 5

Practical tips for complying with Privacy Laws

Practical tips for complying with Privacy Laws

This part covers:

- ePrivacy Law compliance tips, and
- 'Permitted Situations' Quick Reference Guide

Practical tips

Practical steps that a not-for-profit organisation can take to help them comply with Privacy Laws include:		
1.	**Privacy audit**	An organisation should conduct a privacy audit to work out what kind of personal information it collects, uses, stores and discloses. An audit may also show how the not-for-profit organisation manages and safeguards personal information, including how it manages privacy queries and complaints and how it updates, destroys or de-identifies personal information.
2.	**Privacy officer**	An organisation should appoint a person ('privacy officer') to be responsible for developing, implementing and updating its privacy policy, and to be the first point of contact for privacy issues or complaints. Ensure a privacy officer has a dedicated email address (such as *privacy@[organisation].com.au*) to avoid emails relating to privacy issues being missed.
3.	**Privacy policy**	If your organisation falls under the Privacy Laws, you must ensure someone is responsible for preparing, reviewing and updating your organisation's privacy policy. While a not-for-profit organisation's privacy officer should primarily be responsible for the privacy policy, involving administrative and operational staff and volunteers in this process is a good way to make sure the policy reflects current organisational practice and complies with Privacy Laws. A privacy policy should be reviewed regularly (for example, annually) for relevance and updated (for any changes in law or organisational practice).
4.	**Review contracts for impact on privacy law**	A not-for-profit organisation should review its contracts for Privacy Law impact and obligations. In some cases (for example, under Government funding contracts), a not-for-profit organisation may be required to comply with Privacy Laws even if it would otherwise be considered exempt. In other cases, a not-for-profit organisation may outsource services to a third party (for example, fundraising, sponsorship or general services contracts), who may come into contact with or use, collect, store or disclose personal information of the organisation's staff, clients, donors or volunteers. Consider what privacy compliance measures are required in those contracts to make sure obligations flow through to contractors and third parties.

5.	**Privacy checklists, guidelines and manuals**	A not-for-profit organisation should develop privacy checklists, guidelines and manuals to help staff, donors, volunteers and clients understand how the organisation uses, stores, discloses and safeguards personal information. These documents may also outline the organisation's privacy complaint handling procedure and its procedure for handling personal information breaches.
6.	**Data breach response plan**	Have a written internal policy that sets out how your organisation will respond in the case of a breach or suspected breach of privacy.
7.	**Train personnel**	A not-for-profit organisation should train staff, contractors and volunteers on your organisation's privacy policies and carrying out its privacy procedures.
8.	**Transparency**	Ensure your privacy policy, (including details about how users can address privacy issues) is available and accessible.

'Permitted situations' – quick reference guide

The Privacy Act sets out certain 'permitted situations' that allow for collection, use or disclosure of personal information (including sensitive and health information) in special circumstances, (referred to in part 3 of this guide).

An overview of 'permitted situations' most likely to apply to not-for-profit organisations is set out below.

Situation	Applies to	Conditions
Permitted general situations		
Serious threat to life, health or safety	Collection, use or disclosure of: • personal information, or • a government related identifier	• It's unreasonable or impractical to get the person's consent to the collection, use or disclosure, and • your organisation reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any person, or to public health or safety
Unlawful activity or misconduct of a serious nature	Collection, use or disclosure of: • personal information, or • a government related identifier	• Your organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to your organisation's functions or activities has been, is being or may be engaged in, and • your organisation reasonably believes that the collection, use or disclosure is necessary for it to take appropriate action in relation to the matter
Locating a missing person	Collection, use or disclosure of personal information	• Your organisation reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and • the collection, use or disclosure complies with special rules made by the OAIC under section 16A(2) of the Privacy Act

Situation	Applies to	Conditions
Disputes and claims	Collection, use or disclosure of personal information	• The collection, use or disclosure is reasonably necessary for: • the establishment, exercise or defence of a legal or equitable claim, or • the purposes of a confidential alternative dispute resolution process
Permitted health situations		
Provision of a health service	Collection of health information about a person who receives a health service	The information is necessary to provide a health service to the person and either: • the collection is required or authorised under an Australian law (other than the Privacy Act), or • the information is collected in accordance with binding professional confidentiality rules set by competent health or medical bodies
	Collection of health information about a third party	• The health information about the third party is part of the family, social or medical history of the health service recipient • It's necessary for your organisation to collect the health information in order to provide the health service, and • the health information is collected by your organisation from the health service recipient or, if the recipient is physically or legally incapable of giving the information, a responsible person for the recipient
	Disclosure of health information to a person responsible for the health service recipient	• Your organisation provides a health service to the person who the information is about • the recipient of the information is a responsible person for the person who the information is about • the person who the information is about is physically or legally incapable of giving consent to disclosure of the information, or physically can't communicate consent to disclosure • a person providing the heath service for your organisation is satisfied that either: – the disclosure is necessary to provide appropriate care or treatment of the person who the information is about, or – the disclosure is made for compassionate reasons and the disclosure is limited to the extent reasonable and necessary for this purpose, and • the disclosure is not contrary to any wish expressed by the person who the information

Situation	Applies to	Conditions
		is about before they became unable to give or communicate consent, of which the person providing the health service for your organisation is aware or could reasonably be expected to be aware
Use or disclosure of genetic information for the benefit of a family member	Use or disclosure of genetic information	• Your organisation has obtained the genetic information in the course of providing a health service to a person • your organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another person who is a genetic relative of the person who you collected the information from in the course of providing a health service • the use or disclosure is conducted in accordance with approved guidelines as published by the National Health and Medical Research Council **(NHMRC**), and • in the case of disclosure – the recipient of the genetic information is a genetic relative of the person who you collected the information from in the course of providing a health service
Research	Collection of health information	• The collection is necessary for research relevant to public health or safety, the compilation or analysis of statistics relevant to public health or safety, or the management, funding or monitoring of a health service • the purpose cannot be served by collecting de-identified information • it's not practical to get consent from the person who the information is about, and • any of the following apply: – the collection is required under an Australian law (other than the Privacy Act) – the information is collected in accordance with binding professional confidentiality rules set by competent health or medical bodies, or – the information is collected in accordance with approved guidelines as published by the NHMRC. A key requirement of the guidelines is approval by a human research ethics committee (**HREC**)

Situation	Applies to	Conditions
	Use or disclosure of health information	• The use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, • It's not practical to get consent from the person who the information is about • the use or disclosure is conducted in accordance with approved guidelines as published by the NHMRC. A key requirement of the guidelines is approval by a HREC, and • in the case of disclosure – your organisation reasonably believes that the recipient of the information will not disclose the health information, or any personal information derived from the health information

The OAIC has published guides to permitted general situations and permitted health situations.

See Chapter C: Permitted general situations and Chapter D: Permitted health situations of OAIC's APP guidelines. See Chapter C: Permitted general situations and Chapter D: Permitted health situations of OAIC's APP guidelines

Caution- Permitted Situations

If you're not sure whether your collection, use or disclosure of sensitive information falls under any of the permitted situations, you should get legal advice.

justice connect